Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

May 24, 2023

By

Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States. In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction,

maritime, government, information technology, and education sectors. Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible. Microsoft is choosing to highlight this Volt Typhoon activity at this time because of our significant concern around the potential for further impact to our customers. Although our visibility into these threats has given us the ability to deploy detections to our customers, the lack of visibility into other parts of the actor's activity compelled us to drive broader community awareness and further investigations and protections across the security ecosystem.

To achieve their objective, the threat actor puts strong emphasis on stealth in this campaign, relying almost exclusively on living-off-the-land techniques and hands-on-keyboard activity. They issue commands via the command line to (1) collect data, including credentials from local and network systems, (2) put the data into an archive file to stage it for exfiltration, and then (3) use the stolen valid credentials to maintain persistence. In addition, Volt Typhoon tries to blend into normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware. They have also been observed using custom versions of open-source tools to establish a command and control (C2) channel over proxy to further stay under the radar.

In this blog post, we share information on Volt Typhoon, their campaign targeting critical infrastructure providers, and their tactics for achieving and maintaining unauthorized access to target networks. Because this activity relies on valid accounts and living-off-the-land binaries (LOLBins), detecting and mitigating this attack could be challenging. Compromised accounts must be closed or changed. At the end of this blog post, we share more mitigation steps and best practices, as well as provide details on how Microsoft 365 Defender detects malicious and suspicious activity to protect organizations from such stealthy attacks. The National Security Agency (NSA) has also published a Cybersecurity Advisory [PDF] which contains a hunting guide for the tactics, techniques, and procedures (TTPs) discussed in this blog.

As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments. To learn about Microsoft's approach to threat actor tracking, read Microsoft shifts to a new threat actor naming taxonomy.

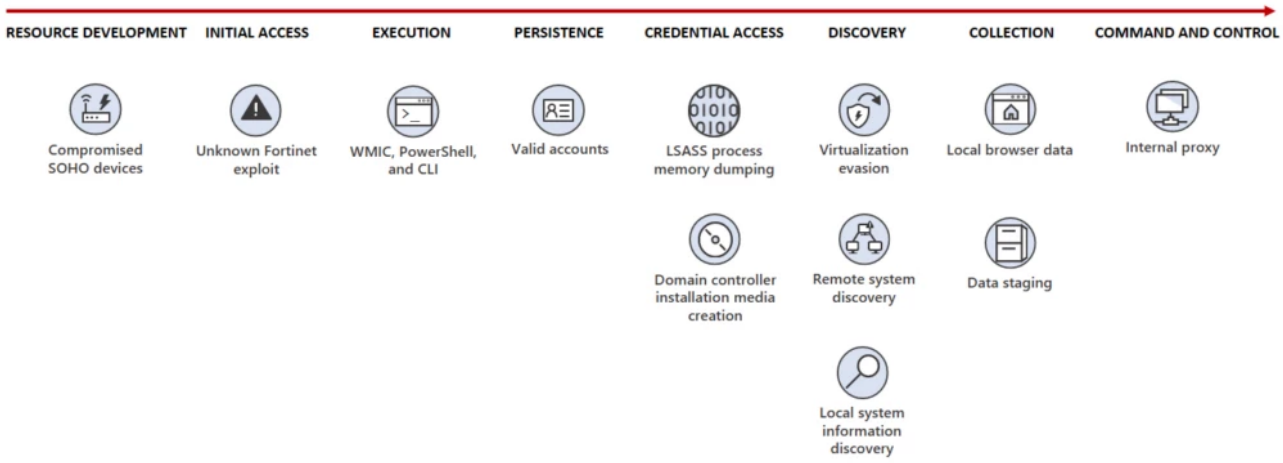

Figure 1. Volt Typhoon attack diagram

Initial access

Volt Typhoon achieves initial access to targeted organizations through internet-facing Fortinet FortiGuard devices. Microsoft continues to investigate Volt Typhoon's methods for gaining access to these devices.

The threat actor attempts to leverage any privileges afforded by the Fortinet device, extracts credentials to an Active Directory account used by the device, and then attempts to authenticate to other devices on the network with those credentials.

Volt Typhoon proxies all its network traffic to its targets through compromised SOHO network edge devices (including routers). Microsoft has confirmed that many of the devices, which include those manufactured by ASUS, Cisco, D-Link, NETGEAR, and Zyxel, allow the owner to expose HTTP or SSH management interfaces to the internet. Owners of network edge devices should ensure that management interfaces are not exposed to the public internet in order to reduce their attack surface. By proxying through these devices, Volt Typhoon enhances the stealth of their operations and lowers overhead costs for acquiring infrastructure.

Post-compromise activity

Once Volt Typhoon gains access to a target environment, they begin conducting hands-on-keyboard activity via the command line. Some of these commands appear to be exploratory or experimental, as the operators adjust and repeat them multiple times.

Volt Typhoon rarely uses malware in their post-compromise activity. Instead, they rely on living-off-the-land commands to find information on the system, discover additional devices on the network, and exfiltrate data. We describe their activities in the following sections, including the most impactful actions that relate to credential access.

Credential access

If the account that Volt Typhoon compromises from the Fortinet device has privileged access, they use that account to perform the following credential access activities.

Microsoft has observed Volt Typhoon attempting to dump credentials through the Local Security Authority Subsystem Service (LSASS). The LSASS process memory space contains hashes for the current user's operating system (OS) credentials.

```
cmd.exe /c powershell -exec bypass -W hidden -nop -E
cgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdAB1A
G0AMwAyAFwAYwBvAG0AcwB2AGMAcwAuAGQAbABsACwAIABNAGkAbgBpAEQAdQBtAHAAIAA1ADUAMg
AgAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAdgBtAHcAYQByAGUALQB2AGgAbwBzAHQ
ALgBkAG0AcAAgAGYAdQBsAGwA
```

Figure 2. Volt Typhoon command to dump LSASS process memory, encoded in Base64

```
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 552
C:\Windows\Temp\vmware-vhost.dmp full
```

Figure 3. Decoded Base64 of Volt Typhoon command to dump LSASS process memory

Volt Typhoon also frequently attempts to use the command-line tool *Ntdsutil.exe* to create installation media from domain controllers, either remotely or locally. These media are intended to be used in the installation of new domain controllers. The files in the installation media contain usernames and password hashes that the threat actors can crack offline, giving them valid domain account credentials that they could use to regain access to a compromised organization if they lose access.

```
wmic /node:[redacted] /user:[redacted]/password:
[redacted] process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp
& ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\tmp\" q q"
```

Figure 4. Volt Typhoon command to remotely create domain controller installation media

```
cmd.exe /c  ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\pro" q q
```

Figure 5. Volt Typhoon command to locally create domain controller installation media

Discovery

Microsoft has observed Volt Typhoon discovering system information, including file system types; drive names, size, and free space; running processes; and open networks. They also attempt to discover other systems on the compromised network using PowerShell, Windows Management Instrumentation Command-line (WMIC), and the *ping* command. In a small number of cases, the threat actors run system checks to determine if they are operating within a virtualized environment.

Collection

In addition to operating system and domain credentials, Volt Typhoon dumps information from local web browser applications. Microsoft has also observed the threat actors staging collected data in password-protected archives.

Command and control

In most cases, Volt Typhoon accesses compromised systems by signing in with valid credentials, the same way authorized users do. However, in a small number of cases, Microsoft has observed Volt Typhoon operators creating proxies on compromised systems to facilitate access. They accomplish this with the built-in *netsh portproxy* command.

```
wmic  /node:[redacted] /user:[redacted] /password:
[redacted] process call create "cmd.exe /c netsh interface portproxy
add v4tov4 listenport=50100 listenaddress=0.0.0.0
connectport=[redacted] connectaddress=[redacted]"

wmic  /node:[redacted] /user:[redacted] /password:
[redacted] process call create "cmd.exe /c netsh interface portproxy
delete v4to4v listenport=50100 listenaddress=0.0.0.0"
```

Figure 6. Volt Typhoon commands creating and later deleting a port proxy on a compromised system

In rare cases, they also use custom versions of open-source tools Impacket and Fast Reverse Proxy (FRP) to establish a C2 channel over proxy.

Compromised organizations will observe C2 access in the form of successful sign-ins from unusual IP addresses. The same user account used for these sign-ins may be linked to command-line activity conducting further credential access. Microsoft will continue to monitor Volt Typhoon and track changes in their activity and tooling.

Mitigation and protection guidance

Mitigating risk from adversaries like Volt Typhoon that rely on valid accounts and living-off-the-land binaries (LOLBins) is particularly challenging. Detecting activity that uses normal sign-in channels and system binaries requires behavioral monitoring. Remediation requires closing or changing credentials for compromised accounts. Suspected compromised accounts or affected systems should be investigated:

- Identify LSASS dumping and domain controller installation media creation to identify affected accounts.
- Examine the activity of compromised accounts for any malicious actions or exposed data.

- Close or change credentials for all compromised accounts. Depending on the level of collection activity, many accounts may be affected.

Defending against this campaign

- Mitigate the risk of compromised valid accounts by enforcing strong multi-factor authentication (MFA) policies using hardware security keys or Microsoft Authenticator. Passwordless sign-in, password expiration rules, and deactivating unused accounts can also help mitigate risk from this access method.
- Reduce the attack surface. Microsoft customers can turn on the following attack surface reduction rules to block or audit some observed activity associated with this threat:

  Block credential stealing from the Windows local security authority subsystem (lsass.exe).Block process creations originating from PSExec and WMI commands. Some organizations may experience compatibility issues with this rule on certain server systems but should deploy it to other systems to prevent lateral movement originating from PsExec and WMI.
  Block execution of potentially obfuscated scripts.
- Harden the LSASS process by enabling Protective Process Light (PPL) for LSASS on Windows 11 devices. New, enterprise-joined Windows 11 (22H2 update) installs have this feature enabled by default. In addition, enable Windows Defender Credential Guard, which is also turned on by default for organizations using the Enterprise edition of Windows 11.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus to cover rapidly evolving attacker tools, techniques, and behaviors such as those exhibited by Volt Typhoon.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat, or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-compromise.

Detection details and hunting queries

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects attempted post-compromise activity. Note, however, that these alerts can also be triggered by threat activity unrelated to Volt Typhoon. Turn on cloud-delivered protection to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block most new and unknown threats.

- Behavior:Win32/SuspNtdsUtilUsage.A
- Behavior:Win32/SuspPowershellExec.E

- Behavior:Win32/SuspRemoteCmdCommandParent.A
- Behavior:Win32/UNCFilePathOperation
- Behavior:Win32/VSSAmsiCaller.A
- Behavior:Win32/WinrsCommand.A
- Behavior:Win32/WmiSuspProcExec.J!se
- Behavior:Win32/WmicRemote.A
- Behavior:Win32/WmiprvseRemoteProc.B

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint alerts with the following titles can indicate possible presence of Volt Typhoon activity.

> Volt Typhoon threat actor detected

The following alerts may also be associated with Volt Typhoon activity. Note, however, that these alerts can also be triggered by threat activity unrelated to Volt Typhoon.

- A machine was configured to forward traffic to a non-local address
- Ntdsutil collecting Active Directory information
- Password hashes dumped from LSASS memory
- Suspicious use of wmic.exe to execute code
- Impacket toolkit

Hunting queries

Microsoft 365 Defender

Volt Typhoon's post-compromise activity usually includes distinctive commands. Searching for these can help to determine the scope and impact of an incident.

Find commands creating domain controller installation media

This query can identify domain controller installation media creation commands similar to those used by Volt Typhoon.

```
DeviceProcessEvents
| where ProcessCommandLine has_all ("ntdsutil", "create full", "pro")
```

Find commands establishing internal proxies

This query can identify commands that establish internal proxies similar to those used by Volt Typhoon.

```
DeviceProcessEvents
| where ProcessCommandLine has_all ("portproxy", "netsh", "wmic", "process call
create", "v4tov4")
```

Find detections of custom FRP executables

This query can identify alerts on files that match the SHA-256 hashes of known Volt Typhoon custom FRP binaries.

```
AlertEvidence
| where SHA256 in
('baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c',
'b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74',
'4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349',
'c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d',
'd6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af',
'9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a',
'450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267',
'93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066',
'7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5',
'389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61',
'c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b',
'e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95',
'6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff',
'cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984',
'17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4',
'8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2',
'd17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295',
'472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d',
'3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642')
```

Microsoft Sentinel

Below are some suggested queries to assist Microsoft Sentinel customers in identifying Volt Typhoon activity in their environment:

Microsoft customers can use the TI Mapping analytics (a series of analytics all prefixed with ‘TI map’) to automatically match the malicious hash indicators (related to the custom Fast Reverse Proxy binaries) mentioned in this blog post. These analytics are part of the Threat Intelligence solution and can be installed from the Microsoft Sentinel Content Hub if not currently deployed. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy.

Indicators of compromise (IOCs)

The below list provides IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protection to identify past related activity and prevent future attacks against their

systems.

Volt Typhoon custom FRP executable (SHA-256):

- baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c
- b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
- 4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
- c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
- d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af
- 9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a
- 450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267
- 93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066
- 7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5
- 389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61
- c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b
- e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95
- 6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
- cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984
- 17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
- 8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2
- d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295
- 472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d
- 3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642